DEPARTMENT OF THE NAVY

CHIEF INFORMATION OFFICER

CAMPAIGN PLAN

September 2007

FOREWORD

In today's Global War on Terror, our Sailors and Marines depend on Information Technology (IT) in more ways than in any war ever fought. During the six months that I served as a Reservist with a Naval Construction Regiment in Iraq, I had a unique view and perspective of the use of IT in theater. While we are doing a superb job at supporting the warfighter, we can do more.

The Secretary of the Navy has challenged the IT community to provide superior Information Management (IM) and IT capabilities to the Department of the Navy (DON) with special emphasis on providing increased security and reliability, while addressing the needs of the warfighter. We will re-focus our efforts to bring improved IT services to the organization in the form of improving our information-sharing capabilities, securing our network, protecting privacy, and ensuring adequate infrastructure, capability, and performance. In coordination with the DON Deputy Chief Information Officer (Navy) and DON Deputy Chief Information Officer (Marine Corps) we will meet these challenges.

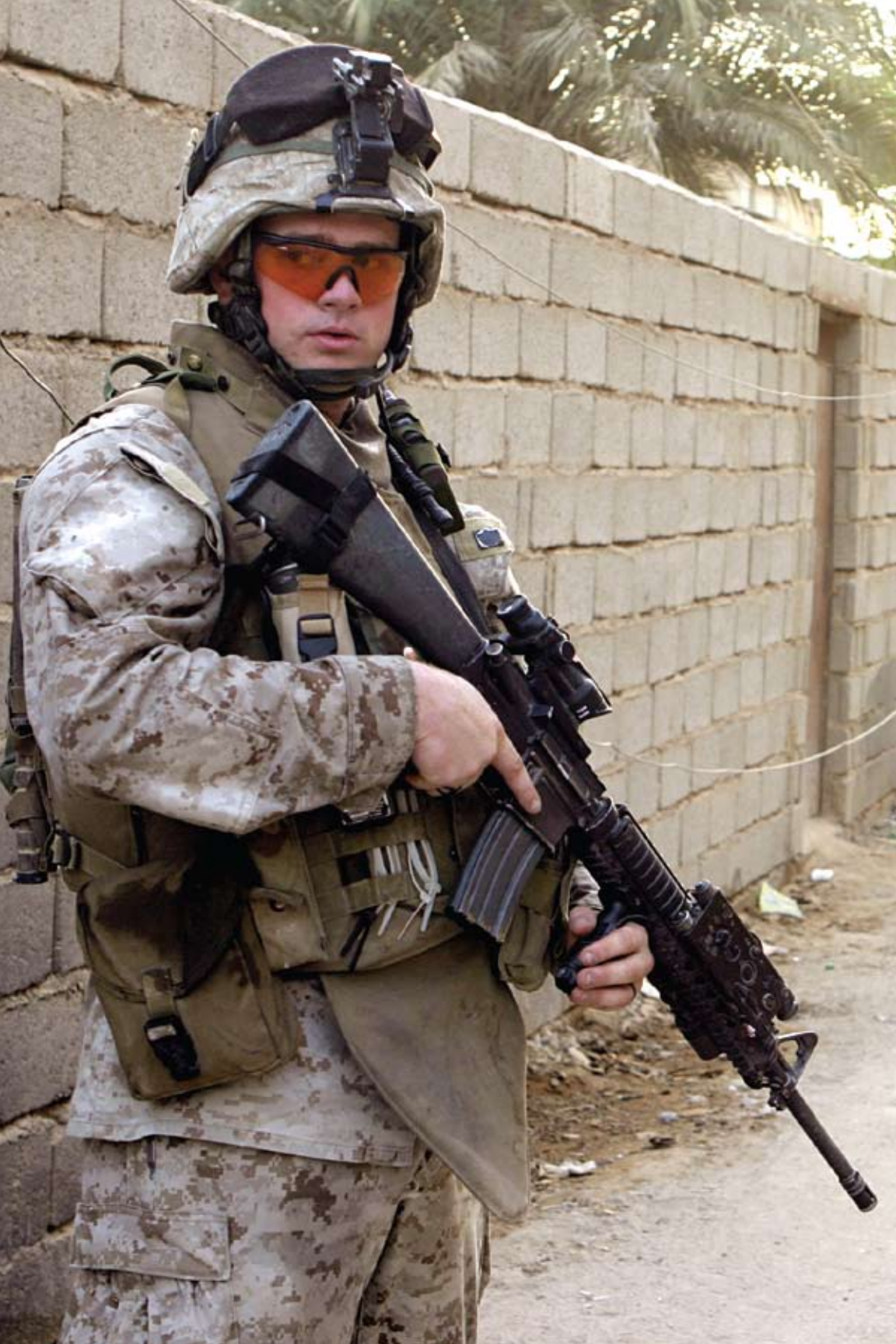
Our goal is to connect the relevancy of our IM and IT initiatives to that of the men and women at the tip of the spear, whether they are aboard a destroyer or deployed to a forward operating base in Iraq. Accordingly, we must bring speed and a sense of urgency to all that we do.

With that goal in mind, this campaign plan represents our major IM and IT focus of effort for the next 500 days. It complements (but does not replace) the DON Information Management and Information Technology Strategic Plan. However, it does include the salient efforts, in line with the strategic plan, that we are undertaking to support the Department while ensuring the needs of the warfighter are met. It delineates the major thrusts that will create the biggest impact within the shortest amount of time.

Robert J. Carey
Department of the Navy
Chief Information Officer

VALUE PROPOSITIONS

1. Provide rapid delivery of key information to the warfighter via secure and reliable electronic means. (Goals 1, 3 & 7)
2. Provide a fast, state-of-the-art information technology infrastructure for delivery of key information and interoperability of computing devices in theater and ashore. (Goals 3 & 4)
3. Maximize the warfighting capabilities of our Sailors and Marines through efficient and effective use of the electromagnetic spectrum. (Goal 5)
4. Provide the warfighter the capability to discover and share knowledge and collaborate electronically to facilitate rapid integration of lessons learned. (Goal 7)
5. Ensure secure, protected information assurance through maximum encryption capability. (Goal 1)
6. Provide assured information delivery, system and network access, and information protection through robust defense-in-depth and defense-in-breadth. (Goal 1)
7. Ensure protection of personally identifiable information through improved reporting processes and employee training and accountability. (Goal 2)
8. Improve processes using Lean Six Sigma methodologies to ensure rapid capability delivery to the warfighter. (Goals 3 & 4)
9. Provide direction and oversight to the IM/IT Workforce Improvement Program. (Goals 1 & 6)
10. Exploit emerging spectrum technology to augment or replace traditional connectivity in support of the deployed and garrison warfighter. (Goal 5)



GOAL 1

Secure the DON IM/IT Infrastructure

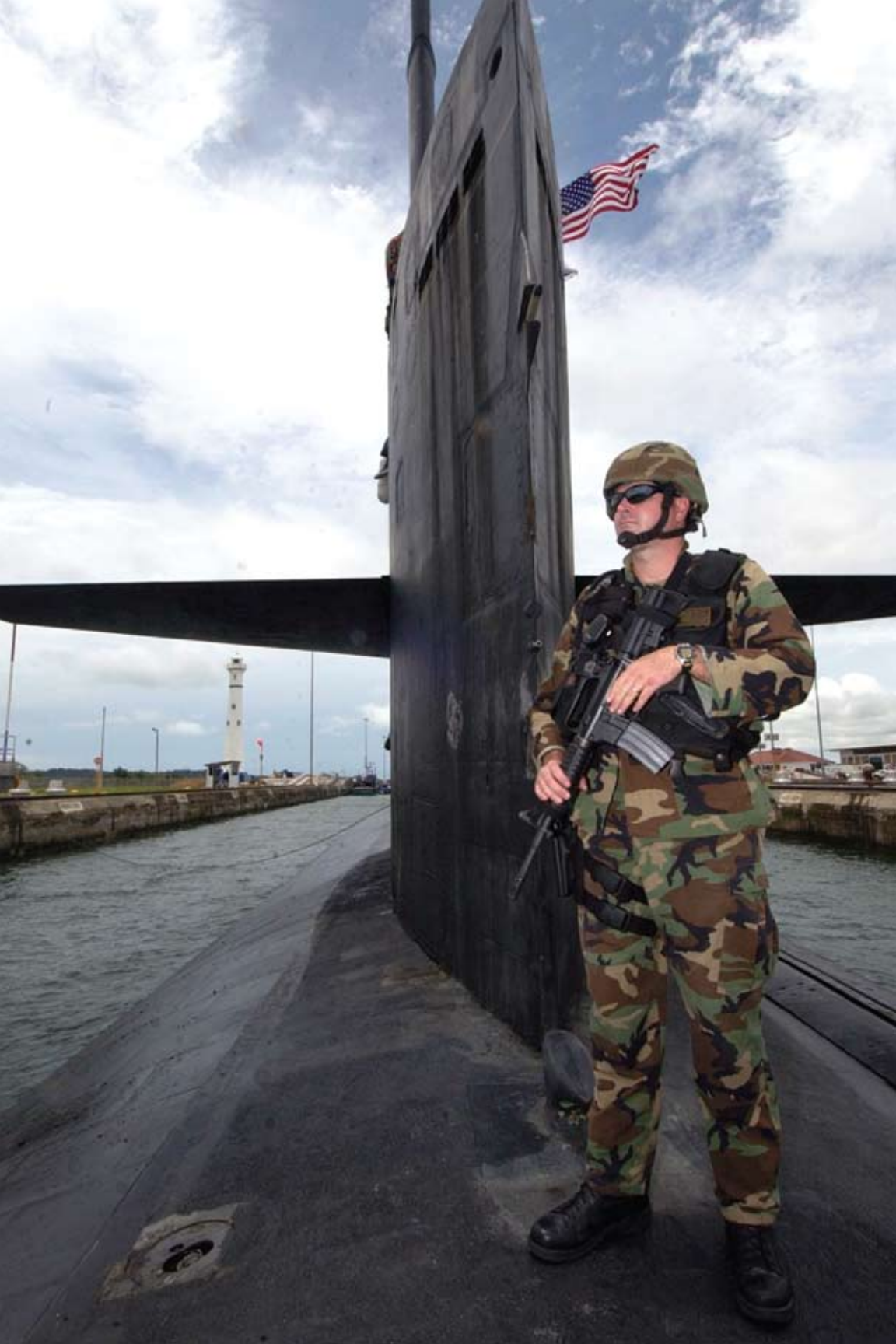
Securing the DON IM/IT infrastructure using defense-in-depth and defense-in-breadth strategies is crucial to the operational capabilities of the warfighter, support personnel, and policymakers. The DON is experiencing increased threats due to increased interconnectivity and interdependency of systems and networks, demanding immediate and swift responses. Our purpose is to protect and defend information contained on DON networks and the systems that carry it to assure confidence and trust in the information necessary for precise decision-making.

TACTICS:

1. Leverage the Department of Defense (DoD)-wide identity management capabilities to centrally manage affiliations of people and network devices.
2. Secure sensitive information residing in DON information systems, mobile assets, and storage media through the implementation of defense-in-depth methodologies such as encryption of data at rest, cryptographic logon, removal of weak network operating systems, and the deployment of state of the art tools to monitor and defend our networks.
3. Strengthen security relationships with the DON industrial base to secure DON sensitive information on contractor networks.
4. Maximize network availability for the warfighter and minimize DON network attacks by ensuring compliance with information assurance vulnerability management, patch implementation, and proper incident handling.
5. Establish a consistent Certification and Accreditation (C&A) process to align with Federal and DoD processes.

OUTCOMES:

- Greater assurance that the DON is protecting IT resources, measured through Federal Information Security Management Act (FISMA) performance measurement scores of 90 percent or better for systems with authority to operate, annual system security reviews, annual security controls testing, and annual contingency plan evaluations.
- Reduction in cost for assessing Information Assurance (IA) controls, measured by successful implementation of a DON policy and process for determining platform IT.
- Reduction in number of successful network intrusions.
- An improved, aligned, and streamlined C&A process within the DON, measured by a 30 percent reduction in cycle time.
- Increased information integrity and confidentiality due to 100 percent encryption of DON data at rest.



GOAL 2

Protect Personally Identifiable Information

Since 1 January 2006, the DON incurred over 100 incidents involving the loss of Personally Identifiable Information (PII), impacting nearly 220,000 Navy and Marine Corps personnel, including retirees, civilians, and their dependents.

PII is defined as, "Information which can be used to distinguish or trace an individual's identity such as their name, social security number, biometrics records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

The Department must focus on training our workforce to enhance awareness of the concerns related to the loss of PII and ensure proper safeguards to protect PII are in place.

TACTICS:

1. Institute policies and programs to change behavior and implement consistent accountability and consequences regarding the suspected and actual loss of PII.
2. Implement ongoing mandatory training of DON personnel to increase PII awareness in order to reduce the number of incidents involving the loss of PII, reduce potential impact on DON personnel (i.e., recovery from potential or actual identity theft), and improve PII incident reporting. Training includes resources available on the Navy's Privacy Web Site and Navy Knowledge Online.
3. Develop and issue a DON data at rest policy and provide the necessary tools to encrypt data at rest on mobile hard drives.
4. Develop a risk management process to categorize and evaluate the severity of PII breaches and provide specific actions to mitigate such incidents.

OUTCOMES:

- All DON personnel are trained in safeguarding and handling PII, including reporting requirements for suspected or actual loss of PII.
- PII breaches are reduced by 90 percent.
- Privacy Impact Assessments are completed for 95 percent of DON systems containing PII.
- Enterprise tools are provided to DON personnel to encrypt data at rest.


ALERT - Missile intercept

GOAL 3

Plan for the IM/IT Environment of the Future

The Department of the Navy's Naval Networking Enterprise–2016 (NNE-2016) initiative is a set of phased activities that will guide the DON toward a net-centric Enterprise environment. NNE-2016 will connect and transform existing DON Enterprise and legacy networks, ashore, in garrison, afloat, and in the field, into a secure, reliable, and globally integrated, net-centric computing and communications Enterprise. NNE-2016 will support the full spectrum of Navy and Marine Corps warfighting and warfighting-support missions and functions.

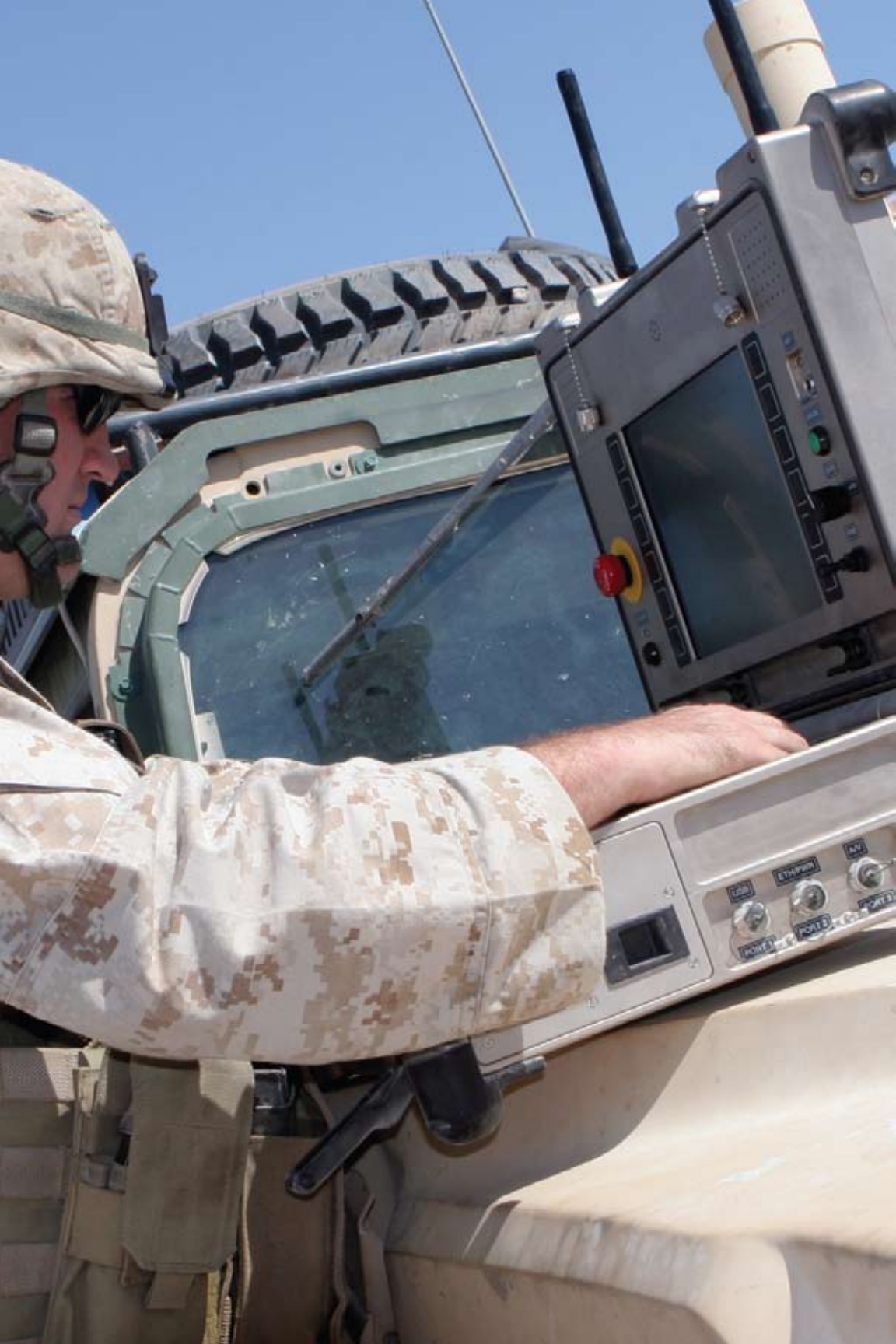
Realizing NNE-2016 will require transforming our people, business processes, and information architecture to support our military forces. The first step in this transformation focuses on gathering the requirements and operational and business justifications for the Next Generation Enterprise Network (NGEN), the replacement for the Department's Navy Marine Corps Intranet (NMCI) contract, which must be in place by September 2010. We must do this as we aggressively provide the Department with the critical security and technology updates to our current network infrastructure and move toward NNE-2016.

TACTICS:

1. Complete the overarching NNE-2016 strategy and Concept of Operations (CONOPS), which will guide the development of NNE-2016 requirements, acquisition strategy, and associated plans, policies, and processes.
2. Develop and implement the security, performance, and reliability enhancements, including technology updates for the current NMCI contract, in order to smoothly transition to the NNE-2016 environment.
3. Ensure appropriate levels of oversight, leadership, and governance are in place to deliver and operate a robust infrastructure for the delivery of operational information to the warfighter and warfighter-support functions.
4. Develop the DON Net-Centric Data Transformation Strategy, which will provide the plan for implementing the DoD vision of net-centricity across the DON.

OUTCOMES:

- NNE-2016 strategy and CONOPS to guide and shape the development and prioritization of the activities required to transition to a net-centric Enterprise environment, including the near-term replacement efforts for NMCI.
- NNE-2016 policy, guidance, and processes necessary to implement the NNE-2016 strategy and CONOPS.
- A consolidated network architecture plan to ensure delivery of the NNE-2016 vision.



GOAL 4

Efficiently Manage Naval IM and IT Investments

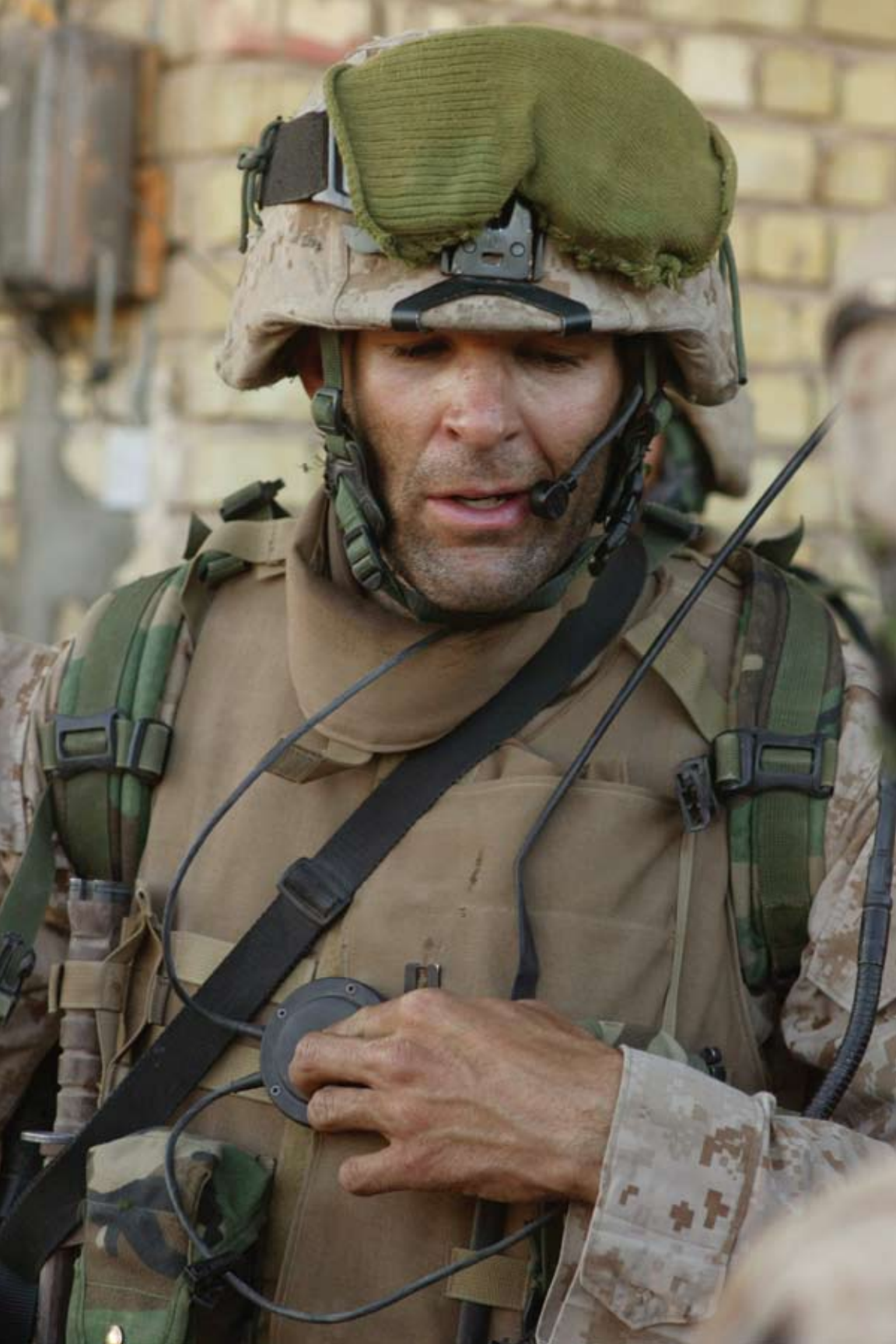
The DON is committed to managing Naval IM and IT investments as efficiently as possible to make resources from efficiencies gained available for warfighting priorities. The DON is working to achieve an optimal mix of investments that delivers required capabilities and eliminates investments that are redundant or not aligned with DoD and DON strategy and policy. We are leveraging the immense buying power of the DoD to reduce the cost of commercial off-the-shelf IT and implement an Enterprise software management process. Additionally, the DON is working to transform and standardize Navy and Marine Corps business processes for key acquisition, financial, human resources, and logistics operations.

TACTICS:

1. Working with the Assistant Secretary of the Navy (Financial Management and Comptroller), Chief of Naval Operations, and Commandant of the Marine Corps, identify a financial management system that supports DON financial management business processes and DoD financial improvement goals.
2. In conjunction with the Assistant Secretary of the Navy (Research, Development and Acquisition), develop and execute policy and processes for centralized management of Enterprise software that will allow the DON to accrue cost avoidance and consolidate licensing for the Navy and Marine Corps.
3. Employ a comprehensive Information Technology Asset Management (ITAM) Plan that will enable the DON to increase the use of commercial software, hardware, and support services.
4. Develop policy that prescribes a DON IT portfolio management process that is aligned with DoD policy and integrated with other decision processes.
5. Embed asset discovery tools that provide visibility into the location and use of DON IT assets, resulting in the reduction of legacy applications, networks, and servers throughout the DON.
6. Execute an Enterprise telecommunications management structure and processes to reduce cost and improve warfighter communications.

OUTCOMES:

- Strategy and supporting business case for a financial application to execute the financial management processes of the Navy/Marine Corps team.
- Streamlined processes for DON IT asset and service procurement at substantial savings over retail and standard GSA prices.
- Policy for a standard, transparent, and repeatable portfolio management process to enable efficient provisioning of IM/IT capabilities to DON warfighters.
- Reinvigorated Functional Area Manager Council that sets DON goals and strategies for continued reduction of legacy applications, networks, and servers.
- Consolidated Enterprise cellular requirements that ensure cost-effective and efficient management of cellular services.
- Policy and processes to manage telecommunications at the Enterprise level.



GOAL 5

Efficiently and Effectively Use Spectrum Technology

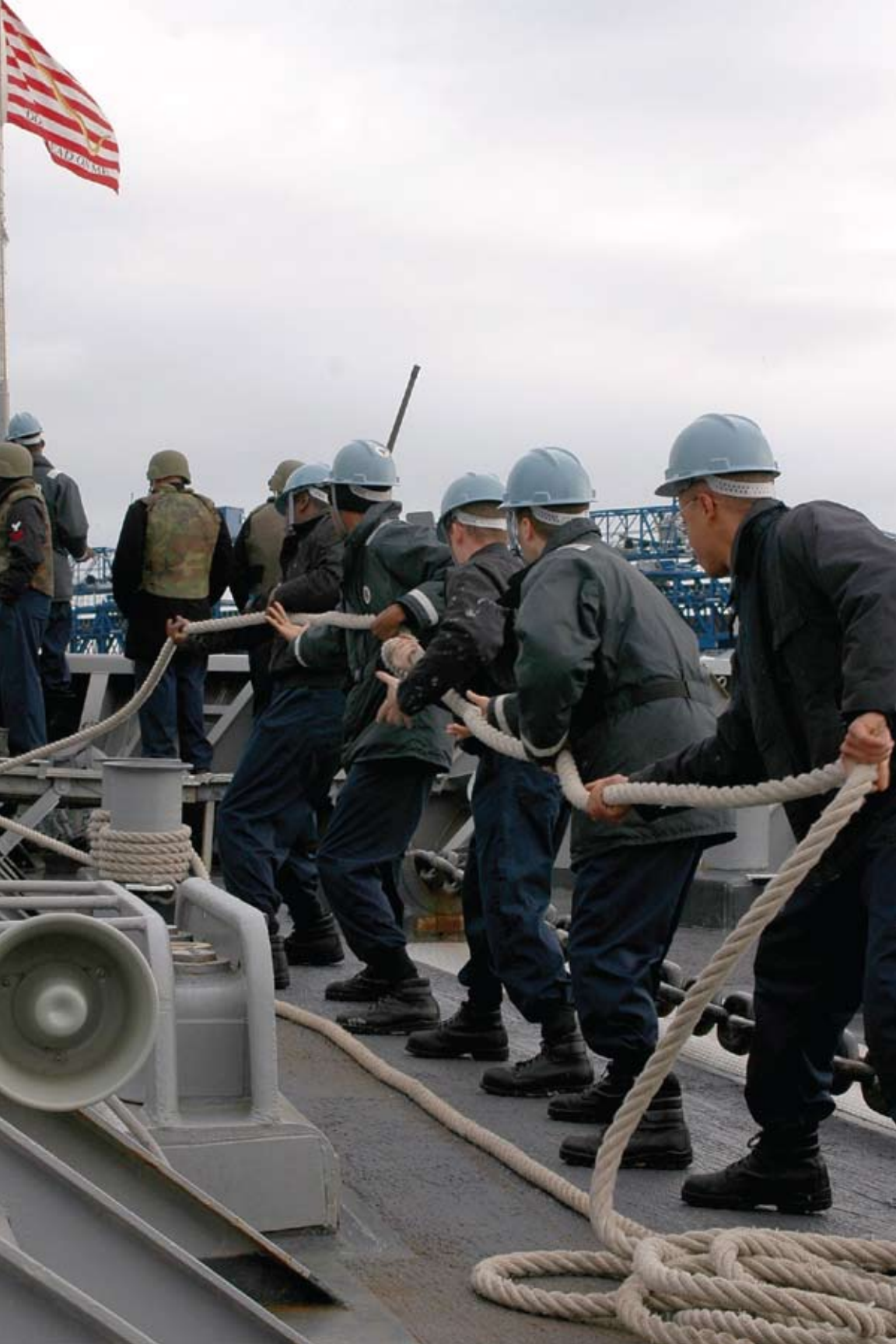
The DON's reliance on the electromagnetic spectrum, which enables safe and reliable wireless communication, intelligence, and sensor capabilities that are integrated with critical weapons capabilities, cannot be overstated. Navy and Marine Corps use of spectrum-dependent systems and equipment has become so pervasive that the DON is now challenged to field new systems that do not cause interference to other systems. In addition to the issue of radio frequency interference, fielding spectrum-dependent equipment that can be used worldwide is extremely complex because nations enact their sovereign right to employ spectrum in their best interests. Consequently, spectrum allocations change from country to country, making the availability of spectrum to support Navy and Marine Corps requirements dependent on the country in which they are operating.

TACTICS:

1. Align spectrum responsibilities within the Department to ensure the DON maximizes the use of finite resources supporting spectrum-dependent systems and equipment.
2. Support the development of automated spectrum decision tools and policy that enable extensive, realistic training and operations that do not degrade naval communications and other spectrum-dependent capabilities.
3. Maintain global leadership in the spectrum arena by supporting the development and acquisition of advanced spectrum technologies, which enable radios to quickly analyze available spectrum resources and efficiently utilize those resources to provide communications superior to those available today.
4. Proactively engage in the international governance of spectrum to advocate global spectrum policy that benefits future Navy and Marine Corps spectrum-dependent capabilities.
5. Apply Lean Six Sigma methods to the DON spectrum supportability determination process to enhance dynamic technology acquisition and speed equipment delivery to the fleet and operating forces.
6. Outline a DON migration strategy for automated spectrum management tools, identifying near-term, mid-term, and far-term requirements.

OUTCOMES:

- Standards and policy for implementation of the next generation of spectrum management tools, which will result in reliable automation and prediction of the electromagnetic environment.
- Standards and policy for employing innovative and adaptive radio technology.
- A DON spectrum supportability determination process that enables rapid acquisition and deployment of spectrum-dependent systems to the warfighter.
- A strategy to deliver spectrum automation tools to support the Naval spectrum contributions to the Global Information Grid.



GOAL 6

Enable DON IM/IT Workforce Excellence

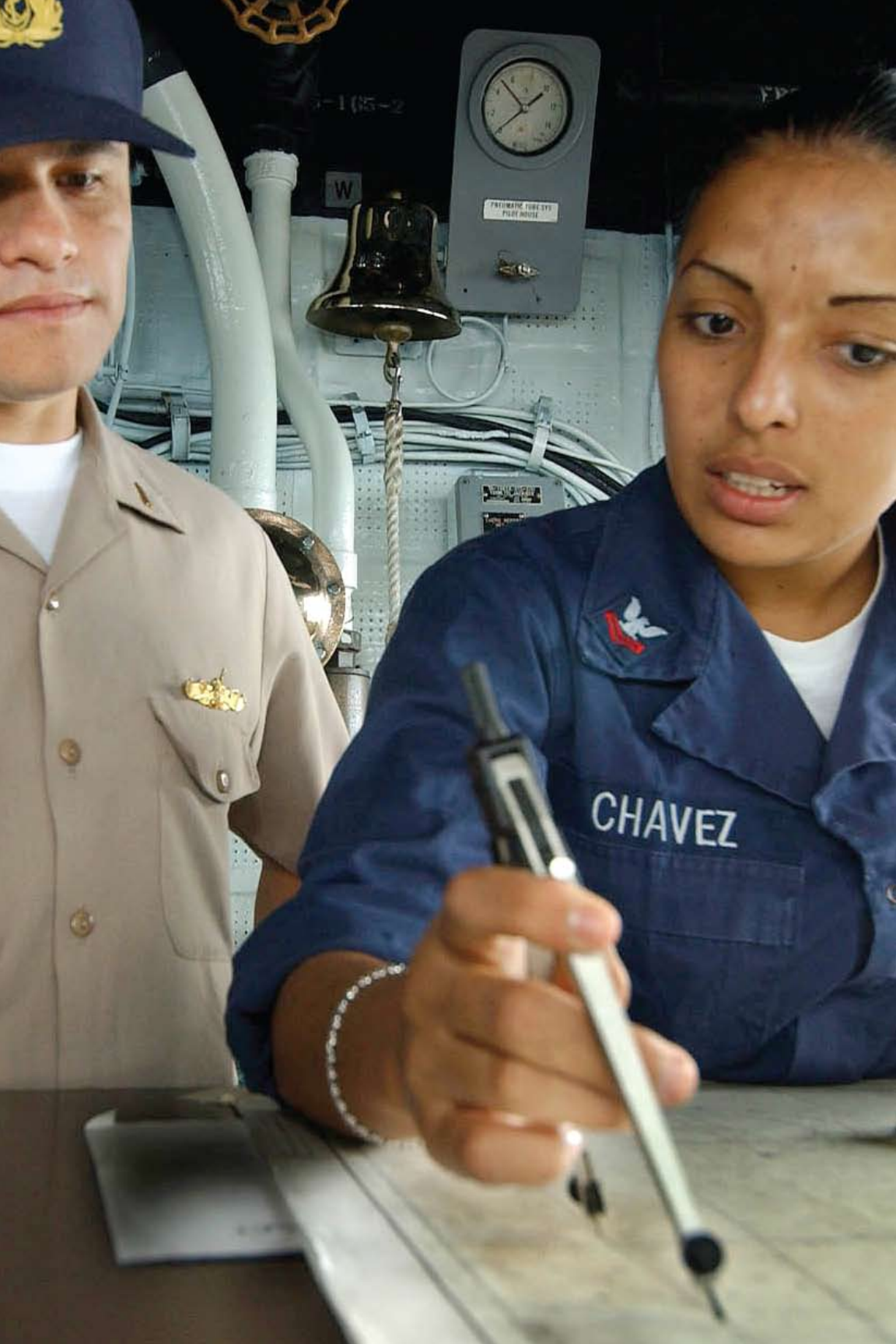
Information Management and Information Technology are essential to carrying out the mission of the Department. As such, the DON IM/IT workforce must be able to utilize current and future technologies to enable a myriad of business processes that support the DON mission. We will focus on efforts required to set strategic direction, identify and define interchangeable IM, IT, IA, and Information Operations (IO) job roles and capabilities, and provide supporting policy required to enhance the capabilities of our Command Information Officers and IT Project Managers.

TACTICS:

1. Develop a DON IM and IT Workforce Strategic Plan that addresses the primary actions related to workforce (IT, IM, IA, IO) manpower, personnel, training, and education areas required to continue to improve the effectiveness of the workforce. As a critical part of this effort, develop the workforce strategy required to support the next generation of networks.
2. Develop, validate, and document the job roles, responsibilities, competencies, and credentials required to support development of a fungible workforce.
3. Develop and promulgate direction for Command Information Officers to include roles, relationships, responsibilities, functions, opportunities, and actions for professional development.
4. Develop and promulgate DON IT Project Manager job roles, relationships, responsibilities, functions, opportunities, and actions for professional development.

OUTCOMES:

- Approved DON IM and IT Workforce Strategic Plan to include a detailed Next Generation Enterprise Network workforce strategy.
- Compendium of DON IM and IT fungible workforce roles, responsibilities, functions, competencies, and credentials.
- Promulgated policy memorandum and formal documentation of the designation of all Echelon II and Major Subordinate Command Information Officers.
- Promulgated DON IT Project Manager Policy Memorandum and valid identification of IT Project Managers.


CHAVEZ

GOAL 7

Improve Knowledge Management Capability

Knowledge Management (KM) integrates people and processes, enabled by technology, to facilitate the exchange of operationally relevant information and expertise to increase organizational performance.

The DON is poised to realize significant benefits from KM by exploiting its capability to improve operational effectiveness. KM concepts and processes, in a variety of implementations and under numerous names, are in broad use across the DON.

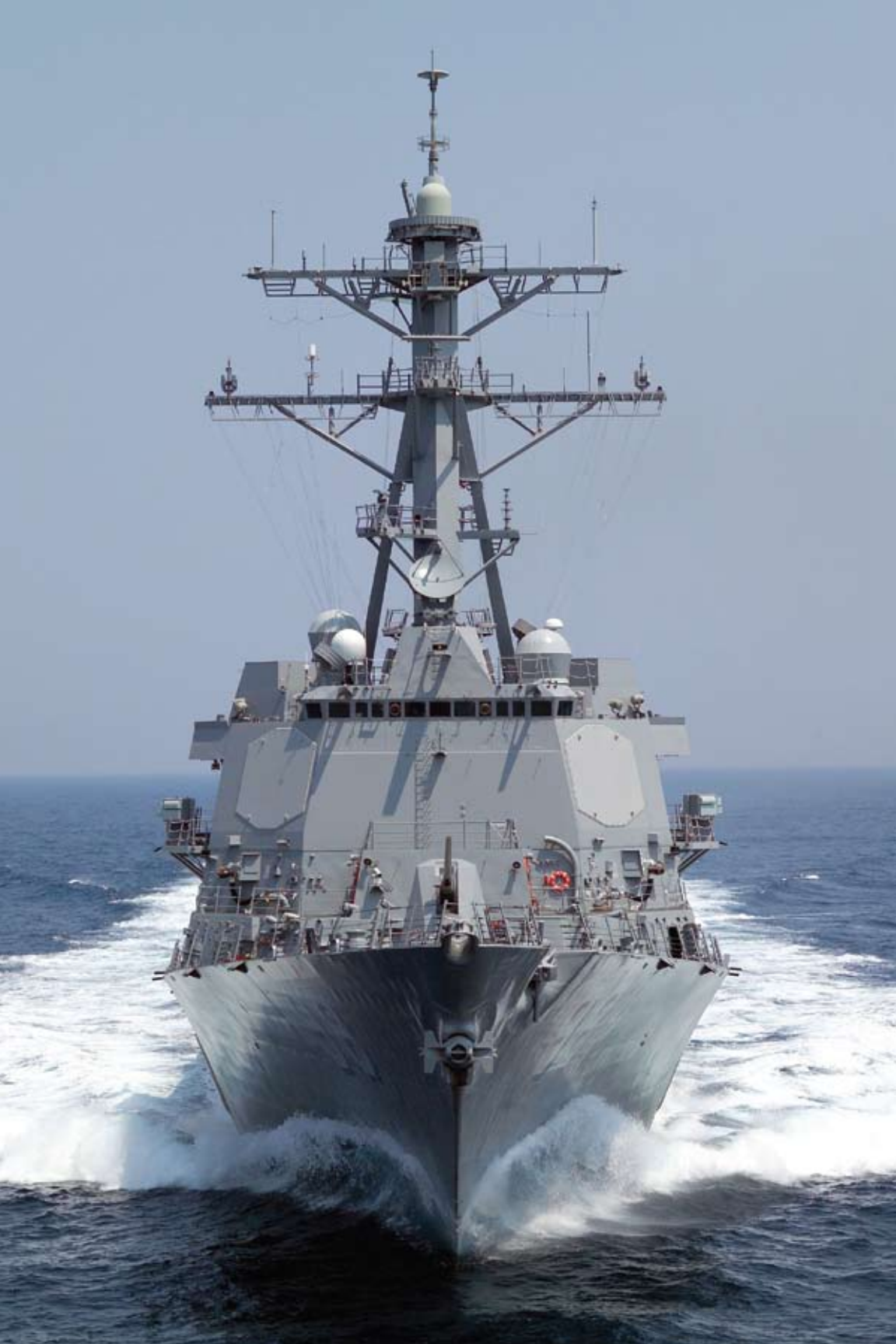
Proper Records Management (RM), especially advances in Electronic Records Management (ERM), provides a rich source of information and allows commands to reconstruct operations and events. Leveraging advances in identity management, information metadata, and data tagging will provide attribute-based and cross-domain knowledge and information sharing.

TACTICS:

1. Building on earlier successes, develop follow-on strategies and guidance for DON knowledge management and attribute-based information sharing.
2. Complete short- and long-range strategies to implement DON Enterprise Content Management (ECM) across the Department to capture, share, and reuse operational information and knowledge for the warfighter and warfighter-support functions.
3. Provide direct assistance to commands implementing KM projects and programs. Work with deployable units to apply KM, train unit personnel on the use of KM tools, and improve the turnover process between the continental United States and theater.
4. Strengthen Departmental records management policy. Develop processes and tools to assist with proper RM and to carry out record information searches.
5. Create an information management value chain that ends in knowledge. (Identity Management + Security + Data Strategies + Content Management + Collaboration Tools = Information Management and Knowledge Management)

OUTCOMES:

- Updated Knowledge Management strategy and guidance.
- Framework for attribute-based information sharing.
- Long- and short-term strategies for ECM.
- Command Records Management Program Guide.
- DON policy and processes for documentary material search, preservation, and production.
- Improved unit level KM expertise.
- Tools and processes for improved turnover process.
- Records discovery process and tools.



DON CIO – *Mr. Robert J. Carey*

DON Deputy CIO – *Mr. John J. Lussier*

DON Deputy CIO (Navy) – *VADM Mark J. Edwards*

DON Deputy CIO (Marine Corps) – *BGen George J. Allen*

DON CIO Contacts

Goal 1

Information Assurance and Network Security Team Leader, (703) 602-6882

Goal 2

Critical Infrastructure Protection and Privacy Team Leader, (703) 602-4412

Goal 3

Director of NGEN Task Force, (703) 602-6847

Goal 4

Director of Investment Management and Performance, (703) 601-0116

Goal 5

Enterprise Services Management Team Leader, (703) 607-5608

Goal 6

IM/IT Workforce Team Leader, (703) 601-0605

Goal 7

Knowledge Management/Records Management and Information Sharing Team Leader, (703) 607-5653

www.doncio.navy.mil

For questions about this Campaign Plan, email webmaster.don_cio.fct@navy.mil

DEPARTMENT OF THE NAVY
CHIEF INFORMATION OFFICER

1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000